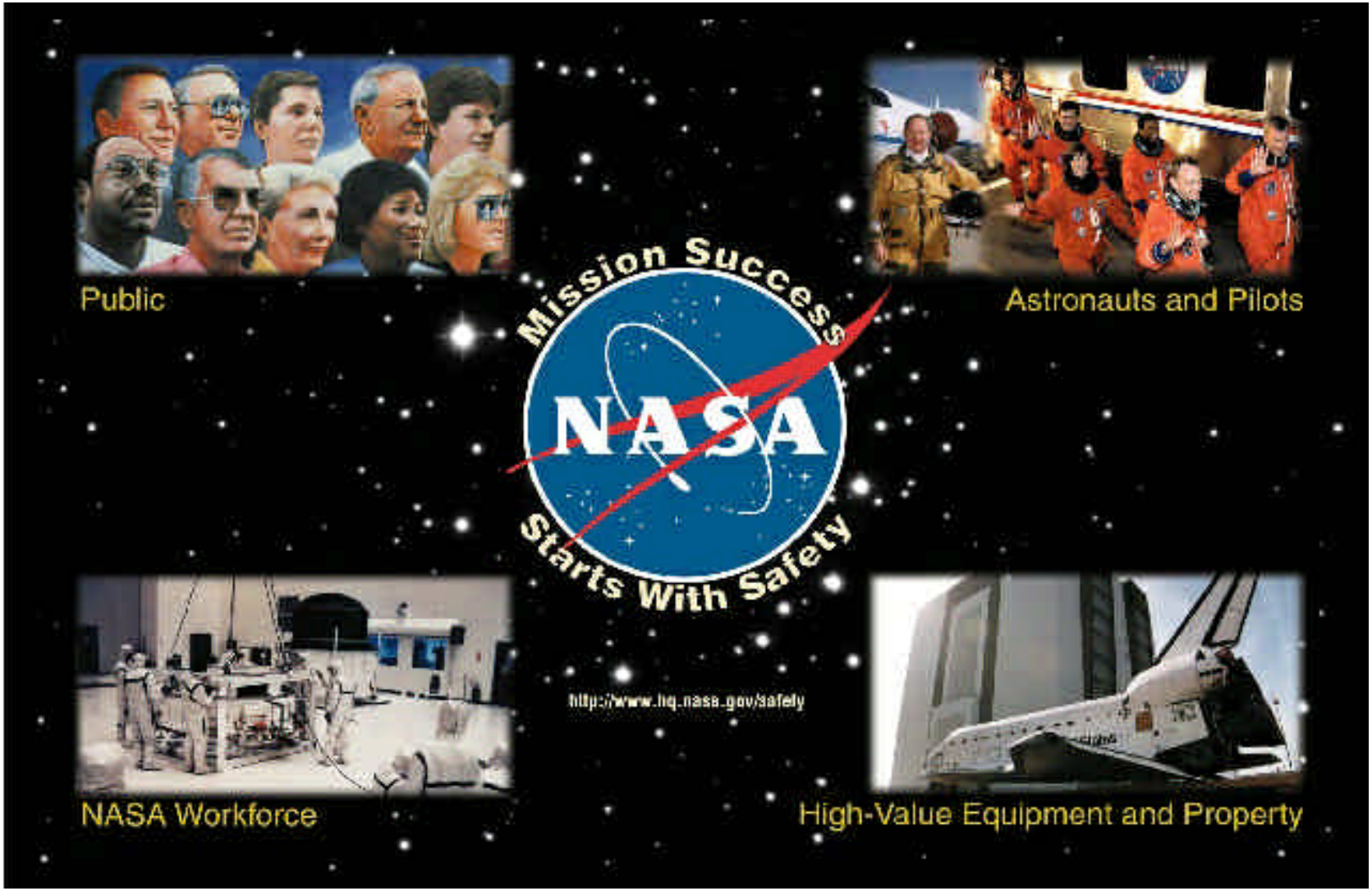
IMPROVING NASA CAPABILITY IN PROBABILISTIC RISK ASSESSMENT

SAFETY DIRECTORS' MEETING
MARCH 21, 2001

Michael G. Stamatelatos, Ph. D.
Manager, Risk Assessment
NASA Headquarters
Office of Safety and Mission Assurance
mstamate@hq.nasa.gov
(202) 358-1668

At NASA, Safety Is #1



NASA Manages Risk on a Daily Basis

⇒ **NASA places public safety, astronaut and pilot safety, personnel safety and property safety at the very top of its priorities**

⇒ **As a technological pioneer, NASA has, explicitly or implicitly, evaluated, accepted and managed risks throughout its existence**

Goals and Objectives	97	02	07	12
1 Fly Safely	Current: 1 vehicle loss in 148 flights	Objective: 1 vehicle loss in 250 flights	Objective: 1 vehicle loss in 325 flights	Objective: 1 vehicle loss in 500 flights

Risk Assessment and Management

Inputs

- Mission Success Criteria
- Technical Data
- Cost
- Schedule
- Management Procedures
- Other

Improved Safety & Performance

Qualitative Risk Assessment

- FMEA
- FTA

Quantitative Risk Assessment

- Initiating Events
- Scenario Modeling (MLD, ESD, ETA, FTA)
- Risk Quantification
- Uncertainty Evaluation

NASA PRA Mission

NASA's PRA mission is to use state-of-the-art PRA methodology to

- ⇒ **ensure mission success**
- ⇒ **improve safety in design, operation, maintenance and upgrade,**
- ⇒ **improve performance and**
- ⇒ **reduce design, operation and maintenance costs**
- ⇒ **support management decisions**

It Was Not Always That Way ...

- ⇒ **Early Apollo program estimate of mission success probability was a disappointing 0.20.**
- ⇒ **However, between 1969 and 1972, 6 out 7 successful Apollo missions demonstrated 0.86 mission success probability.**
- ⇒ **This discrepancy caused dissatisfaction with PRA at NASA**
- ⇒ **October 29, 1986 - The "Investigation of the Challenger Accident" by the Committee on Science and Technology of the House of Representatives criticized NASA for not "*estimating the probability of failure of the various [Shuttle] elements.*"**
- ⇒ **January 1988 - In the "Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management," the Slay Committee recommended that *"probabilistic risk assessment approaches be applied to the Shuttle risk management program at the earliest possible date."***

PRA Returns to NASA

- ⇒ **Between 1987 and 1995, some fifteen PRA studies were performed for NASA**
- ⇒ **In July 1996, NASA Administrator Dan Goldin requested *"a tool to help base (Shuttle) upgrade decisions on risk."***
- ⇒ **In October 1997, an early version of the NASA Quantitative Risk Assessment System (QRAS) was demonstrated to the Administrator.**
- ⇒ **In February 1998, Version 1.0 of QRAS was baselined.**

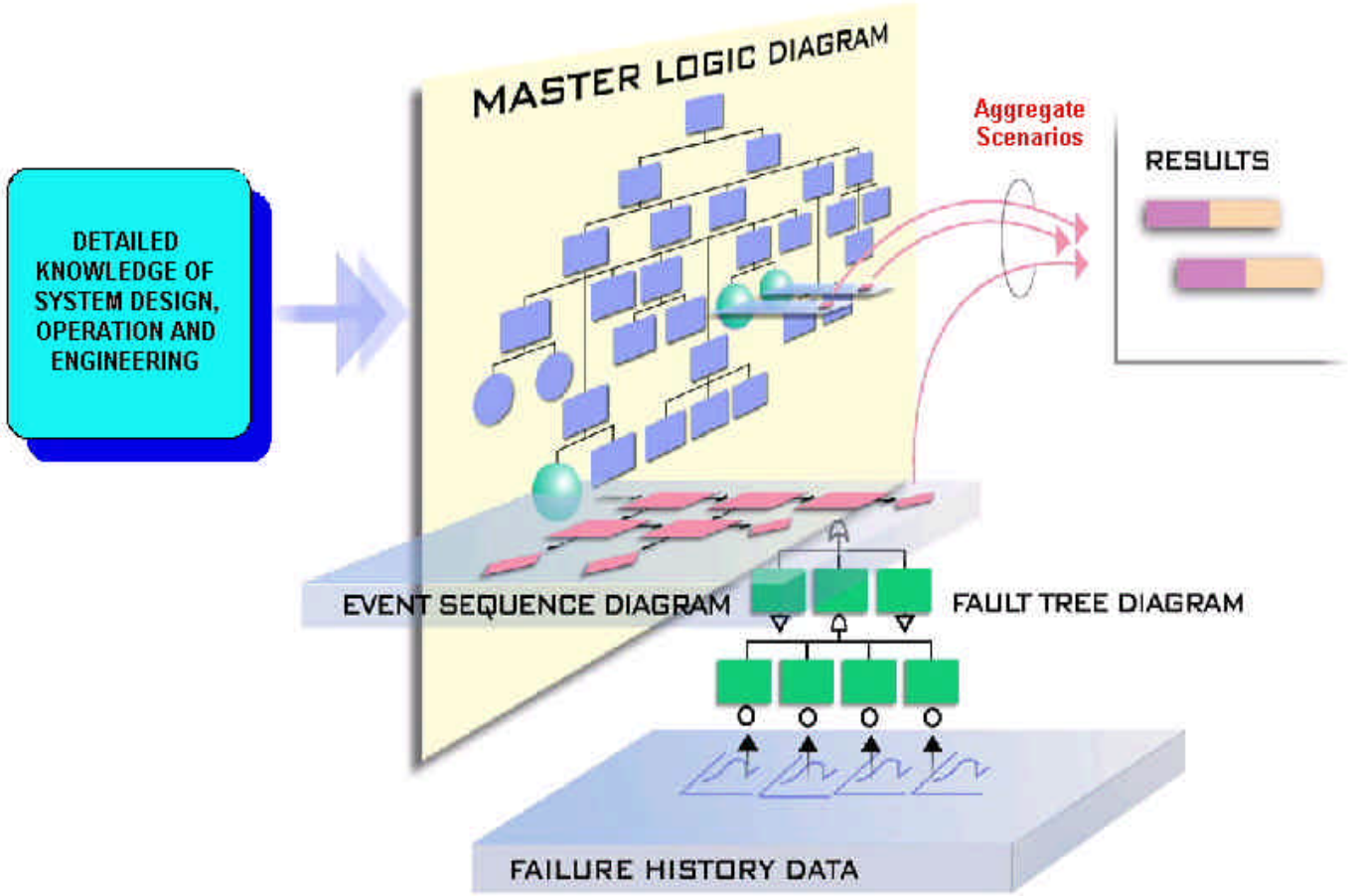
Unfortunately, the PRA efforts during this PRA revival era have found little understanding and usefulness at NASA because important basic ingredients were missing

NASA Acquiring Proven Keys to Success

- **In-house expertise** to perform, manage and use PRAs to make sound decisions
- **In-house ownership and corporate memory** of PRA methods, tools, databases and results
- **Transfer of PRA technology** to in-house personnel and managers who are the ones who need to manage, oversee, understand, and use PRA to make sound management decisions

I CANNOT EMPHASIZE ENOUGH THE IMPORTANCE OF THESE THREE KEY ELEMENTS TO SUCCESS !!!

PRA Methodology Summary



NASA's Full-Scope Scenario-Based PRA Methodology

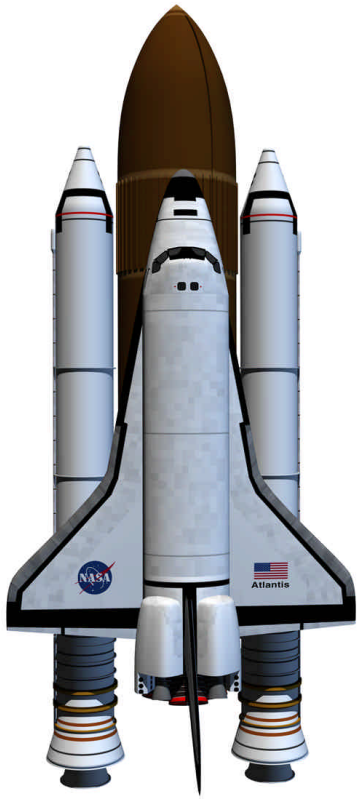
1. Identification of end-states of interest (related to PRA purpose)
2. System familiarization ("as-is" information) and data collection
3. Identification, selection, screening of initiation events, or IE, (may require high-order logic model; e.g., master logic diagram or MLD)
4. Definition and modeling of all scenarios linking each initiating event to the end states, using event sequence diagrams (ESD), or event trees (ET)
5. Modeling of pivotal events, the ET branch points; e.g., using fault trees (FT)
6. Risk quantification for each pivotal event and each scenario and risk aggregation for all like end states
7. Full uncertainty analysis and sensitivity analysis as needed
8. Risk importance ranking for risk reduction

NASA's Unique PRA Methodology Needs

- ⇒ **Broad range of programs: Conceptual non-human rated science projects; Multi-stage design and construction of the International Space Station; Upgrades of the Space Shuttle**
- ⇒ **Risk initiators that vary drastically with type of program**
- ⇒ **Unique design and operating environments (e.g., microgravity effects on equipment and humans)**
- ⇒ **Multi-phasing approach in some scenario developments**
- ⇒ **Unique external events (e.g., micro-meteoroids and orbital debris)**
- ⇒ **Unique types of adverse consequences (e.g., fatigue and illness in space)**
- ⇒ **Different considerations for human reliability (e.g., astronauts vs. other operating personnel)**
- ⇒ **Greater importance of software reliability**
- ⇒ **Specialized database needs**

Space Shuttle PRA

- **Johnson Space Center and Marshal Space Flight Center have been modeling their Shuttle elements, the orbiter and the propulsion system, respectively.**
- **Space Shuttle Program has begun to factor risk into their Upgrades Program.**

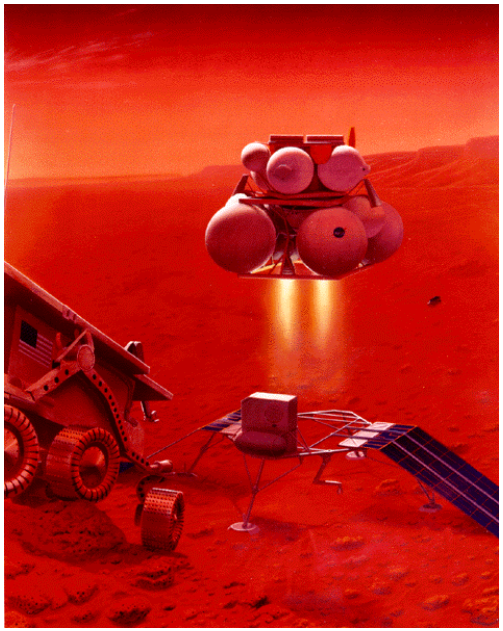


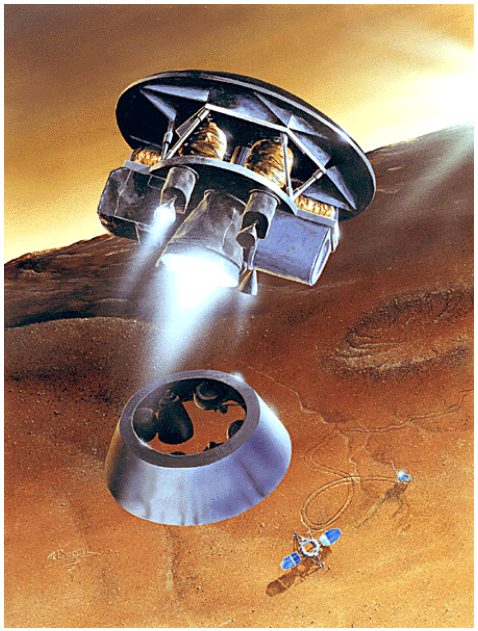
International Space Station PRA

- **1999 -- The NASA Advisory Council recommended, the NASA Administrator concurred, and the ISS Program initiated a PRA.**
  - **First portion of PRA (through Flight 7A) delivered in 2000; Second portion (through Flight 10A) expected in 2001.**
- **Objectives of ISS PRA:**
  - **Provide a quantitative estimate of ISS operations risk**
  - **Provide a model for future ISS safety decision-support activities**
  - **Provide a model for safety related operations planning**
  - **Provide a model for trading marginal safety enhancements versus cost**

Mars Sample Return Mission

- ⇒ **Mission must meet a Planetary Protection Program (PPP) criterion of <10^{-6} probability of Earth contamination upon return of sample**
- ⇒ **PRA is used to evaluate mission compliance with the PPP criterion**

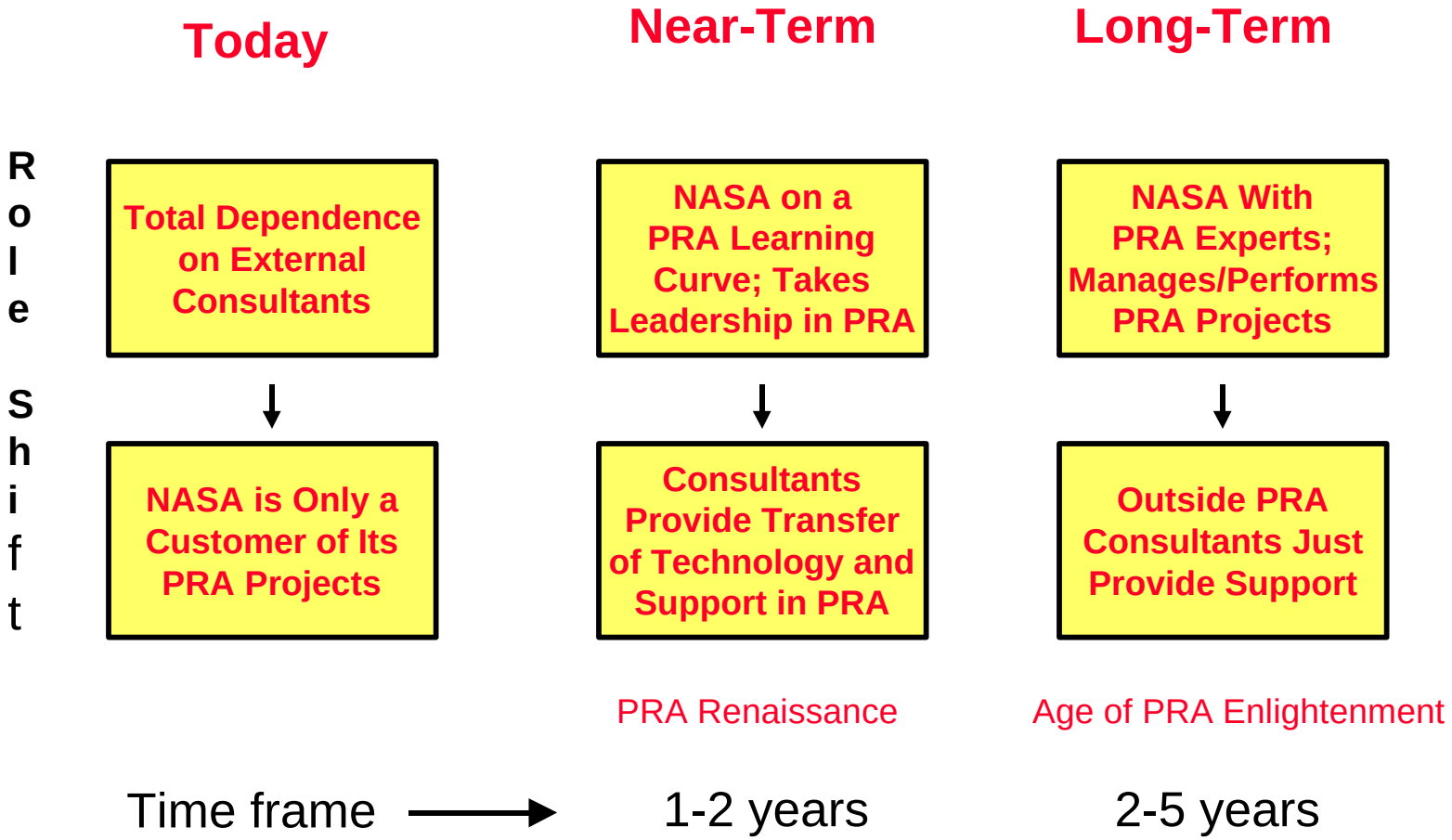




NASA PRA Vision

Develop and maintain a world-class in-house capability to perform, manage, and use Probabilistic Risk Assessment (PRA) methods for the benefit its personnel and programs and, in general, for the benefit of our nation

NASA PRA Capability Growth Model



NASA PRA Accomplishments

Many PRA accomplishments were made by NASA especially over the past twelve months:

- **Policy**
- **Procedures Guide**
- **Training**
- **Computer Tools**
- **Information Exchange**
- **Cooperation with other Government Agencies**

PRA Policy

- Developed draft PRA policy
- Policy recognizes broad range of NASA programs/projects and different needs for PRA application
- Policy recommends when and to what extent PRA should be implemented in NASA programs/projects
- Policy is currently under review
- Publish in June 2001

PRA Policy

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS		NASA PROGRAM/PROJECT (Classes and/or Examples)
Human Safety & Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return
		White House Approval (PD/NSC-25)	Nuclear payload (e.g., Cassini, Ulysses, Galileo)
	Human Space Flight		International Space Station
			Space Shuttle
			Crew Return Vehicle
Mission Success (for non-human rated missions)	High Strategic Importance		Mars Program
	High Schedule Criticality		Launch window (e.g., planetary missions)
	Higher-Cost Missions (>$100M)		Earth Science Missions (e.g., EOS)
			Space Science Missions (e.g., SIM)
			Technology Demonstration and Validation (e.g., EO-1)
	Lower-Cost Missions (<$100M)		Earth Science Missions (e.g., QUICKSCAT)
			Space Science Missions (e.g., HESSI)
			Technology Demonstration and Validation (e.g., Deep Space 1)

PRA Procedures Guide

- NASA is developing a state-of-the-art Procedures Guide for Aerospace applications by PRA practitioners
- It consists of a main document and appendices
- This draft will be available at the end of March 2001
- The final version of the guide will be available later this year

Awareness & Practitioner Training

- NASA developed PRA awareness and practitioner courses and workshops
- Management awareness training was conducted at HQ and at NASA centers
- A one-week workshop on PRA Fundamentals for practitioners at KSC was conducted by INEEL at the end of January 2001
- A new NASA-developed one-week PRA methodology course for practitioners will be conducted at HQ during the first week in April 2001

PRA Computer Tools

- NASA acquired SAPHIRE PRA computer program and adopted it as “baseline” PRA computer program for the Agency
- SAPHIRE PRA training was conducted at HQ and Centers; 90 NASA personnel have been trained on SAPHIRE to date
- QRAS Version 1.6, an integrated PRA computer program, to be delivered in the March-April 2001 timeframe
- Dynamic fault tree program (ASSAP) was developed for NASA and is being tested

PRA Information Exchange

- In October 2000, NASA organized PRA information exchange workshop at HQ involving broad Agency participation
- Additional workshops for PRA information exchange are planned for 2001 and future
- NASA-wide working groups for application of PRA technology are being contemplated

Cooperation with Other Government Agencies

- NASA is cooperating with NRC in PRA
- NASA started cooperation with ESA on PRA policy and procedures
- NASA is cooperating with ESA in hosting a joint conference on risk management and payload safety (November 2001)
- NASA has initiated cooperation with NASDA on PRA methodology and database

This Is Only the Beginning

NASA is continuing its aggressive approach of using Probabilistic Risk Assessment as a decision assistance tool for engineering and management applications